MULTIMEDIA UNIVERSITY®

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2017/2018

ECE3246 – SECURITY & CRYPTOGRAPHY

(CE, ME)

12 MARCH 2018
2.30 P.M – 4.30 P.M
(2 Hours)

INSTRUCTIONS TO STUDENT

1. This examination paper consists of 6 pages including the cover page with 4 questions only.
2. Attempt **any THREE** out of **FOUR** questions. All questions carry equal marks and the distribution of the marks for each question is given.
3. Please print all your answers in the Answer Booklet provided.

Question 1

a) Describe your understanding of the following *security concepts*:

(i) **oracles** [3 marks]

(ii) **indistinguishability** [3 marks]

b) (i) Discuss the reasons why a *block cipher* is not suitable for achieving the security property of **integrity** (INT). [3 marks]

(ii) Discuss the reasons why a *hash function*'s structure is designed to be **iterative** in nature. [3 marks]

c)

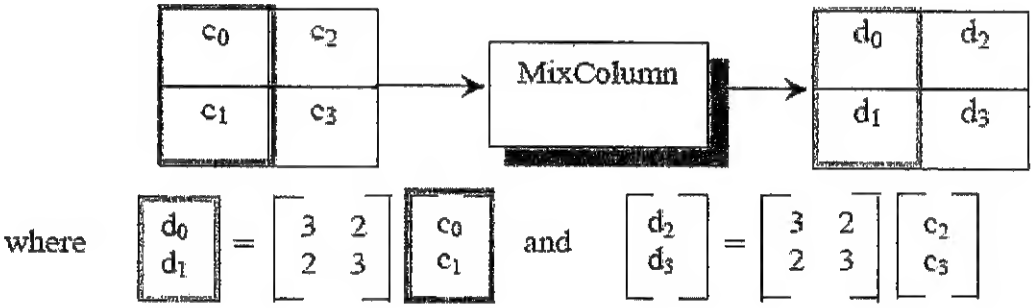

Figure 1 MixColumns operation of Mini-AES

Recall the *MixColumns* (MC) and *AddRoundkey* (AR) operations of Mini-AES. MC is performed as per Figure 1, i.e. each column of the input matrix is taken as a column vector to be matrix multiplied with a constant matrix (3,2;2,3). Meanwhile, for an input matrix (d_0,d_1,d_2,d_3) of four nibbles, AR simply exclusive-ORs the matrix elements with a round key (r_0,r_1,r_2,r_3) of also four nibbles.

Given an input (c_0,c_1c_2,c_3) going first into AR, show by use of appropiate symbols and notations, how you can **express the output** (e_0,e_1e_2,e_3) after going through the operations of *AR then followed by MC*.

Note: the order of "AR then MC" is different from that discussed in lectures. [8 marks]

Continued...

Question 2

a) Describe your understanding of the *authentication factors* of '**what you know**' and '**what you are**', then **compare** which is more secure in terms of what is required by an attacker in order to attack them. [3+3 marks]

b) Consider an adversary against a *hash function*. Discuss how an adversary could **interact** with the algorithm, and then discuss what **goal(s)** that the adversary would want to achieve against this type of function.

[2+4 marks]

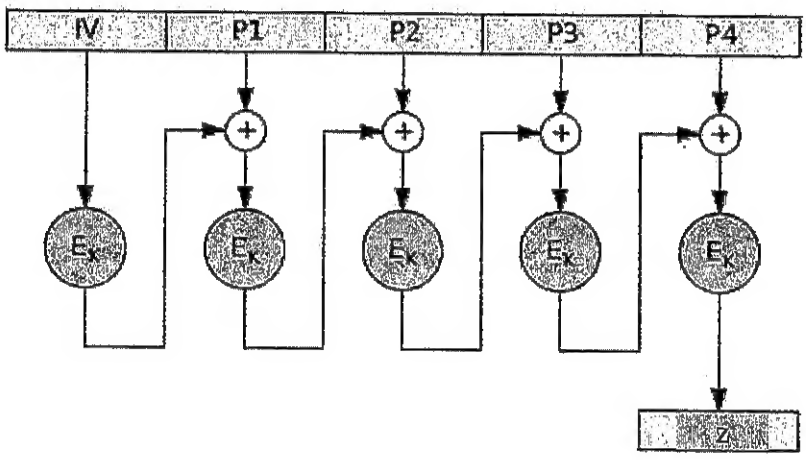

Figure 2 [sourced from http://www.cs.rit.edu/~ark]

c) Figure 2 illustrates an *operation mode* for a *block cipher E*.

(i) Discuss the reasons why this operation is **not invertible**.

[4 marks]

(ii) Discuss what happens at the receiver side when an attacker has mounted a **replacement attack** to replace block P3 while the other blocks remain unchanged. [4 marks]

Continued...

Question 3

a) (i) Describe the basic gist behind how the *ElGamal encryption* scheme overcomes the **deterministic problem** exhibited by textbook RSA. [3 marks]

(ii) Discuss how the **performance** is affected by the requirement in *public key cryptography* to ensure that doing with one key can only be undone by another key.

[3 marks]

b) The *RSA public key cipher* performs encryption defined as follows

$$c = m^e \bmod n$$

where c is the ciphertext, m the plaintext, e the public key and n the modulus, and decryption is defined as

$$m = c^d \bmod n.$$

Given that the public key e is 37, private key d is 13, and modulus n is 40; show how a ciphertext $c = 2$ can be **decrypted.** [6 marks]

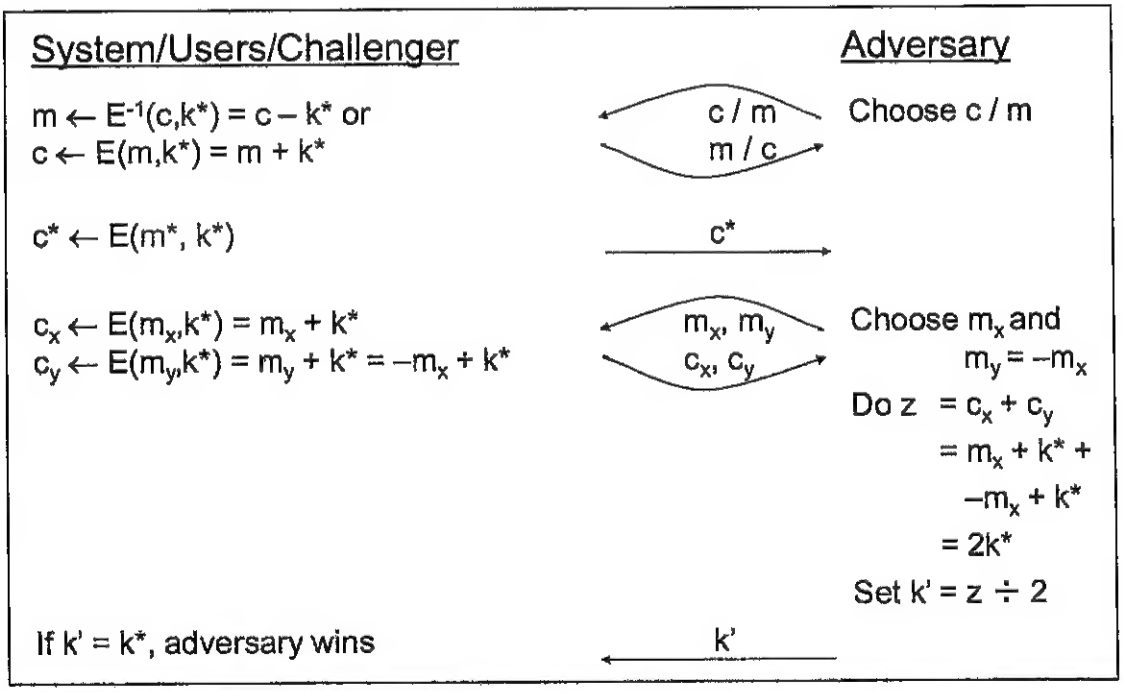

Figure 3

Continued...

c) Figure 3 shows an attack by an adversary against the *AddCipher symmetric encryption* in the securiyy model called the *key-recovery against chosen-ciphertext attacks* (KR-CCA) model.

(i) Describe which parts of the model consider adversarial **oracles.**

[3 marks]

(ii) Discuss the basic strategies to **prevent** this attack from being successful.

[5 marks]

Question 4

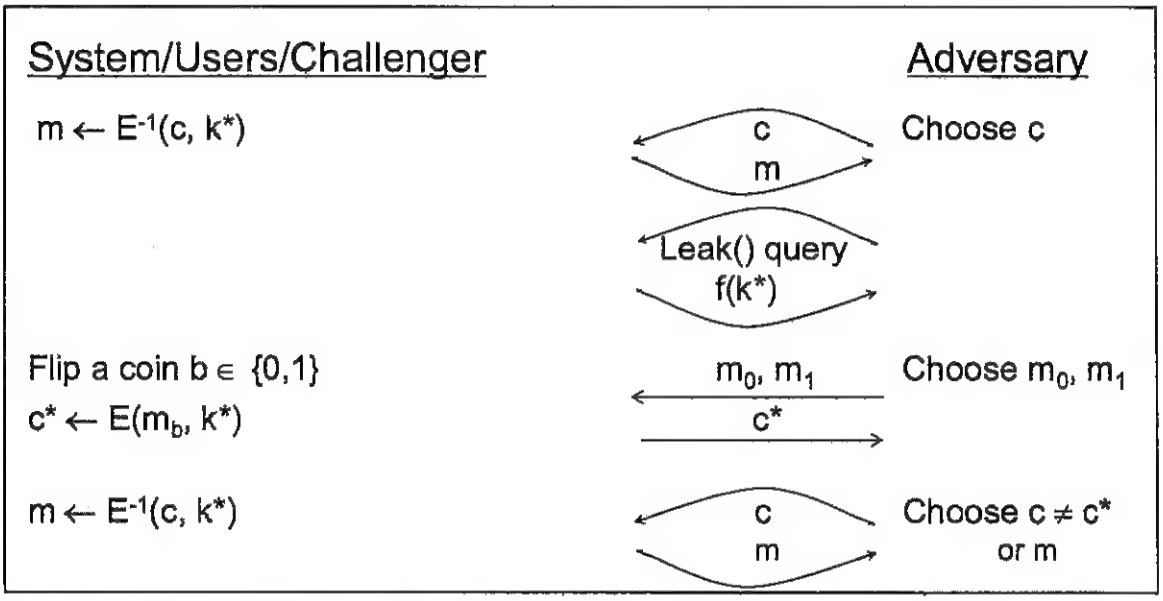

Figure 4

a) Figure 4 shows a type of *compromise* of secret data when security techniques such as encryption are implemented in real life system.

(i) Describe example **situations in real life** where this type of compromise might occur. [3 marks]

(ii) From the Figure 4, discuss what is modelled by the value of the **coin flip b.**

[3 marks]

Continued...

b)

(i) Describe the **adversarial goal** when the security of *digital signature* schemes is considered. [3 marks]

(ii) Describe the basic **differences** between *intrusion resilience* and *intrusion resistance*.

[3 marks]

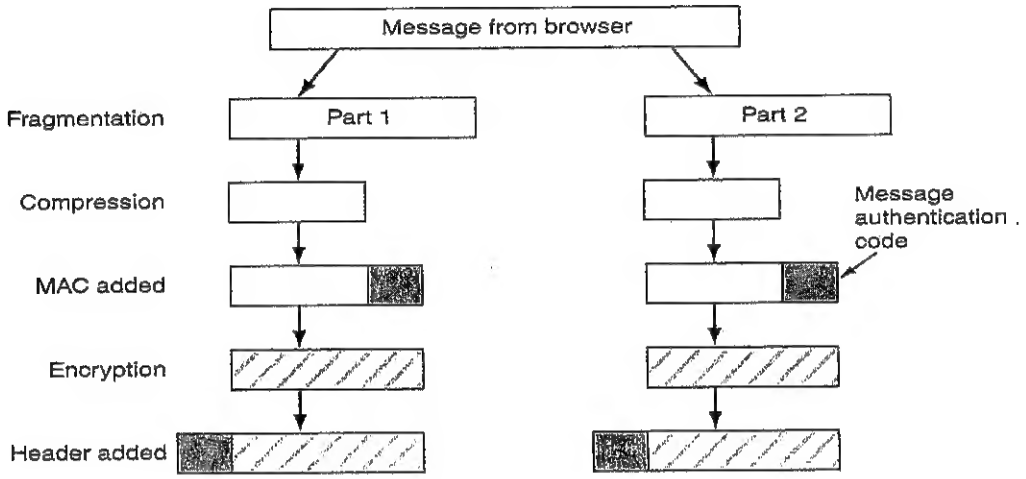

Figure 5

c)

Figure 5 shows the *Transport Sub-protocol* of the Secure Sockets Layer (SSL), in particular the operations performed at the sender side. More precisely, for fragment m1, the following is computed and sent to the recipient:

$z = \text{header} \,||\, \text{Encrypt}\,(\,\text{Compress}(m1) \,||\, \text{MAC}(m1)\,)$

(i) Note that MAC is performed before Encryption; this approach is so-called authenticate-then-encrypt (AtE). Describe the alternative approach of **encrypt-then-authenticate** (EtA). [5 marks]

(ii) Discuss what happens at the **receiving side** for the alternative approach of encrypt-then-authenticate (EtA).

[3 marks]

End of Paper